UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/710,350	07/02/2004	Andre KRAMER	2006579-0444	4349

69665 7590 07/09/2008

CHOATE, HALL & STEWART / CITRIX SYSTEMS, INC.
TWO INTERNATIONAL PLACE
BOSTON, MA 02110

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

NOTIFICATION DATE	DELIVERY MODE
07/09/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTDOCKET@CHOATE.COM

Office Action Summary	Application No.	Applicant(s)	
	10/710,350	KRAMER, ANDRE	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in reply to amendment after non-final filed on March 4th 2008. New claims 30-33 are added. Independent Claims 1, 29 and dependent claim 27 are amended. Thus claims 1-33 are pending of which 4 of them are independent claims, namely claims 1, 15, 26 and 29.

2. The amendment made to the dependent claim 27 overcomes the objection set forth in the previous office action. Thus the objection is overcome and is withdrawn.

Priority

3. This application does not claim priority of an application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **07/02/2004.**

Response to Arguments

4. Applicant's argument/s filed on March 4th 2008 have been fully considered but are moot in view of new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. **Claims 1-33** are rejected under 35 U.S.C. 103(a) unpatentable over Publication, IBM Technical Disclosure Bulletin, title, "Administrative Role Configuration with Control Lists" TDB-ACC-NO: NB9112110 (hereinafter referred as **IBM**) (Publication date: December 1, 1991)(Submitted in the pervious office action) in view of Laksono (hereinafter referred as

Laksono) (U.S. Publication No. 2003/0046584 A1) (filed on: September 5, 2001)

6. **As per independent claims 1, 26 and dependent claims 30, 32 IBM discloses a method for providing secure access to applications** *[Page 3, lines 32-34*] **(***This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article)*

the method comprising the steps of:

- **Receiving a request from a user to execute an application** *[Page 4, lines 19-20 and page 4, lines 16-17[On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");*

- **Determining a minimal set of computing privileges necessary for the user to use the requested application** *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with* ***the least privilege mechanism*** *described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article. The submitted specification on paragraph 0005 disclosed the following. "The principle of* ***least privilege ensures that an application runs with the minimal amount of permissions*** *necessary to accomplish its assigned tasks".)***; and**

- **Invoking an execution environment for the user having the determined set of privileges** *[Page 4, lines 16-18 and page 4, lines 18-21] (On page 4, lines 16-18, the following has been disclosed. "any method of executing the command will 'work' - that is, the* ***invoker will acquire the correct privileges****." Furthermore on page 4, lines 18-21, the following has been disclosed. "this method allows privilege to be acquired whether the command is executed by* ***direct user invocation****, by shell script or via system call or subroutine.")*

Though IBM teaches "the least privilege mechanism" as shown above it does not explicitly disclose "determining a minimal set of computing privileges necessary for the user to use the requested application"

However, in the same field of endeavor **Laksono on paragraph 0032**, discloses the following.

"The process begins at step 80, where a hand held device of the multimedia system transmits a remote control/monitoring request to a server of the multimedia system" and this meets the limitation recited as "Receiving a request from a user to execute an application" because the hand held device as disclosed on paragraph 0024 could be any kind of device including a laptop which can be operated by the user.

And Laksono on paragraph 0034 discloses the following.

"The process proceeds to step 84 where the server determines remote control and monitoring privileges of the hand held device. The determination of the privileges will be described in greater detail with reference to FIG. 8. The process continues at step 86 where the server **determines whether the hand held device has at least a minimum level of remote control and monitoring privileges."** and this meets the limitation recited as "Determining a minimal set of computing privileges necessary for the user to use the requested application"

And finally Laksono on paragraph 0035 discloses the following.

"If the hand held device has a minimal level of privileges, the process proceeds to step 90, where the server processes the remote control/monitoring request with respect to at least one of the plurality of clients to produce operational monitoring data."

And this meets the limitation recited as "Invoking an execution environment for the user having the determined set of privileges"

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as **"determining a minimal set of computing privileges necessary for the user to use the requested application"**

as per teachings of **Laksono** into the method as taught **by Ibm** in order to build a secure monitoring system and enhancing the security or "the access control" of the system. [See Laksono at least paragraph 0010]

7. **<u>As per independent claims 15 & 29, and dependent claims 16, 31, 33</u> IBM discloses an application server system providing secure access to hosted applications,** *[Page 3, lines 32-34] (On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation recited as "providing secure access to hosted application)* ***the system comprising:***

- **A policy based decision system receiving a request from a user to execute an application** *[On page 3, lines 32-34, the following for instance has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article and this meets the limitation of a policy based decision system. Furthermore, on page 3, lines 34-page 4, line 1, the following has been disclosed. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted and this also meets the limitation recited as "***A policy based decision system***") receiving a request from a user to execute an application** *(Page 3, lines 32-34, Page 4, lines 19-20 and page 4, lines 16-17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine." and on page 4, lines 16-17, see "any method executing the command")*;

and determining a minimal set of privileges required by the user to

execute the application *[Page 3, lines 29-34] (The disclosed mechanism works in conjunction with the least privilege mechanism described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*;

- **An account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for the user having the determined set of privileges;** [See page 4, lines 12-23] (On page 4, lines 12-23, the following has been disclosed. "*Since the commands themselves do not enforce policy, the* ***administrator who controls privilege assignment is free to configure the system roles in whatever manner is appropriate for the local system"****, and this meets "the account administration service". Furthermore the following has been disclosed- "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file, any method of executing the command will 'work' - that is, the invoker will acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined" and this meets

the limitation "an account administration service in communication with said policy based decision system, the account administration service invoking an execution environment for the user having the determined set of privileges".) and

A connection manager in communication with said policy based decision system *[See again page 4, lines 19-20 and 4, lines 16-17 "the entity/interface receiving client's request/execution command meet the limitation of connection manager and this interfaces between the user and the Privilege Control List system/policy based decision system"]*, **said connection manager receiving from a client system an RDP request by the user to execute the application** *[Page 4, lines 19-20 and page 4, lines 16-17][On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or subroutine."" and on page 4, lines 16-17, see "any method executing the command");***and transmitting to said policy based decision system an identification of said user and an identification of said application**.*[See on page 3, lines 32-page 4, line 1 and page 4, lines 16-23] (On page 3, lines 32-page 4, the following has been disclosed. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article. A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted. This meets the limitation recited as*

"policy based decision system based on identification of said user". Furthermore, the following has been stated. "This mechanism is also compatible with existing practice. Because the privilege is associated directly with the program file and this meets the limitation recited as "policy based decision system based on identification of said application", any method of executing the command will 'work' - that is, the invoker will acquire the correct privileges. Unlike the second mechanism described above, this method allows privilege to be acquired whether the command is executed by direct user invocation, by shell script or via system call or subroutine. - Lastly, this mechanism allows privilege to be granted based on arbitrary combinations of identifiers, thus increasing the flexibility with which the system privilege control policy can be defined

Though IBM teaches "the least privilege mechanism" as shown above it does not explicitly disclose "determining a minimal set of computing privileges necessary for the user to use the requested application"

However, in the same field of endeavor **Laksono on paragraph 0032**, discloses the following.

"The process begins at step 80, where a hand held device of the multimedia system transmits a remote control/monitoring request to a server of the multimedia system" and this meets the limitation recited as "Receiving a request from a user to execute an application" because the hand held device as disclosed on

paragraph 0024 could be any kind of device including a laptop which can be operated by the user.

And Laksono on paragraph 0034 discloses the following.

"The process proceeds to step 84 where the server determines remote control and monitoring privileges of the hand held device. The determination of the privileges will be described in greater detail with reference to FIG. 8. The process continues at step 86 where the server **determines whether the hand held device has at least a minimum level of remote control and monitoring privileges."** and this meets the limitation recited as "Determining a minimal set of computing privileges necessary for the user to use the requested application"

And finally Laksono on paragraph 0035 discloses the following.

"If the hand held device has a minimal level of privileges, the process proceeds to step 90, where the server processes the remote control/monitoring request with respect to at least one of the plurality of clients to produce operational monitoring data."

And this meets the limitation recited as "Invoking an execution environment for the user having the determined set of privileges"

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as **"determining a minimal set of computing privileges necessary for the user to use the requested application"**

as per teachings of **Laksono** into the method as taught **by Ibm** in order to build a secure monitoring system and enhance the security or "the access control" of the system. [See Laksono at least paragraph 0010]

8. **As per dependent claims 2-3 and 17-18 the combination of IBM and Laksono discloses a method as applied to claims above. Furthermore, IBM discloses the method, comprising the further step of: returning an identifier for the execution environment to the requesting user.** *[Page 4, lines 18-23 and page 3, lines 34-page 4, lines 4] (For instance on page 4, lines 18-23 the following has been disclosed. "This mechanism allows privilege to be granted based on* ***arbitrary combinations of identifiers****, thus increasing the flexibility with which the system privilege control policy can be defined." Furthermore on page 3, lines 34-page 4, lines 4, the following has been disclosed. "A Privilege Control List (PCL) consists of an unordered set of Privilege Control Entries. Each entry consists of a list of typed identifiers and a set of privileges. The list of typed identifiers defines the circumstances under which the privileges will be granted, and the format of the data structures permits extension to arbitrary types of identifiers")*

9. **As per dependent claim 4 the combination of IBM and Laksono discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (a) comprises receiving an HTTP-based request from a user to execute an application.** *[Page 4, lines 19-20 and page 4, lines 16-17[On page 4, lines 19-20, see "the command is executed by direct user invocation by shell script or via system call or*

subroutine."" and on page 4, lines 16-17, see "any method executing the command");

10. **<u>As per dependent claims 5-8, 20-25 and 27-28 the combination of IBM and Laksono</u> discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (b) comprises accessing a policy-based decision system to determine a minimal set of computing privileges necessary for the user to use the requested application.** *[Page 3, lines 29-34 and page 3, lines 35- page 4, line 4] (The disclosed mechanism works in conjunction with* ***the least privilege mechanism*** *described in (*), which describes mechanism for associating a set of discrete privileges with a file. This is extended by means of a Privilege Control List mechanism, which works in much the same way as the Access Control List mechanism described in the following article.)*

11. **<u>As per dependent claims 9 and 19 the combination of IBM and Laksono</u> discloses a method as applied to claims above. Furthermore, IBM discloses the method, further comprises determining a minimal set of computing privileges necessary for the user to use the requested application based, at least in part, on a role assigned to the user.** *[page 4, lines 12-14* **]***[See at least the title, "administrative role configuration" with privilege control lists and see on page 4, lines 12-14, "Since the commands themselves do not enforce policy, the administrator who controls privilege assignment is free to configure the system roles in whatever manner is appropriate for the local*

system" and on page Page 3, lines 29-34 and page 3, lines 35- page 4, line 4, see "the least privilege mechanism")

12. **<u>As per dependent claims 10-13 the combination of IBM and Laksono</u> discloses a method as applied to claims above. Furthermore, IBM discloses the method, wherein step (c) further comprises creating an execution environment for the user having the determined set of privileges. [***Page 4, lines 16-18 and page 4, lines 18-21] (On page 4, lines 16-18, the following has been disclosed. "any method of executing the command will 'work' - that is, the **invoker will acquire the correct privileges**." Furthermore on page 4, lines 18-21, the following has been disclosed. "this method allows privilege to be acquired whether the command is executed by **direct user invocation**, by shell script or via system call or subroutine.")*

13. **<u>As per dependent claims 14 the combination of IBM and Laksono</u> discloses a method as applied to claims above. Furthermore, IBM discloses the method, further comprising the steps of initiating a connection with a client system associated with the user. [***Page 4, lines 16-18 and page 4, lines 18-21] (See for instance, command is executed by **direct user invocation)***

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

For instance the NPL reference cited and attached in this office action see reference U (IEEE article published on 2003 from Department of

computer science, Virginia Tech) on page 4, first column, 4th paragraph discloses the following.

"THE LEAST Privilege access principle dictates that a request to a resource should be served with the minimum amount of privilege required to render the requested service. Furthermore on the same paragraph the following has been disclosed. "The ability to specify exactly what privilege is to be used with a specific access permits a subject to define access requests with the minimum privileges required."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

06/25/2008

/Samson B Lemma/
Examiner, Art Unit 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132